

Betriebssysteme

Bitlocker

Bitlocker kann verschlüsselt werden durch:

- TPM-Modul (transparent)
- TPM + PIN oder enhanced PIN
- USB-Key
- Kennwort
- RecoveryKey

Per Default verschlüsselt Bitlocker nur mit AES-128.

Per GPO kann man AES CBC 256 aktivieren. (Performance)

Computerkonfiguration -> Administrative Vorlagen -> Windows Komponenten -> Bitlocker-Laufwerksverschlüsselung

-> «Verschlüsselungsmethode und Stärke wählen» - **aktivieren**

-> «Verschlüsselungsmethode für Wechsellaufwerke wählen» - **AES CBC 256-Bit**

Bitlocker per GPO aktivieren:

Computerkonfiguration -> Administrative Vorlagen -> Windows Komponenten -> Bitlocker-Laufwerksverschlüsselung -> Betriebssystemlaufwerke

-> «Konfigurieren von TPM-Systemstart-PIN» und «Require Start-PIN Bei TPM» wählen

Status abfragen: CMD-Befehl

manage-bde -status

Preboot-PIN-Abfrage aktivieren:

manage-bde -protectors -add c: -TPMandPIN

PIN ändern:

manage-bde -changePIN c:

PIN-Abfrage wieder deaktivieren:

manage-bde -protectors -add c: -TPM

Betriebssysteme

Bitlocker suspendieren für HD-Wartung, Bios-Updates u.ä. (Bsp. LW X):

- per GUI in Bitlocker Verwaltung: Schutz anhalten / fortsetzen
- per PowerShell: **Suspend-BitLocker -MountPoint "X:"**
- per PS, nur System-LW, für 1-9 Neustarts, 0= ewig: **Suspend-BitLocker -MountPoint "<drive letter>:" -RebootCount <restarts>**
- per CMD: **manage-bde -protectors -disable X:**
oder **manage-bde -protectors -disable X: -rc 5** (pausiert für 5 Neustarts)

Siehe auch: [Verschlüsselung](#)

Ext. Links:

- Administrator.de [Wissenssammlung Bitlocker](#) ,
- [dateibasierter Bitlockerprotektor zu Recovery- und Supportzwecken](#)

Eindeutige ID: #1243

Verfasser: Uwe Kernchen

Letzte Änderung: 2021-08-11 19:45